

1 ENGROSSED HOUSE
2 BILL NO. 2669

By: Derby of the House

and

Brinkley of the Senate

3
4
5
6
7 An Act relating to information technology; amending
8 62 O.S. 2011, Section 34.32, as amended by Section
9 364, Chapter 304, O.S.L. 2012 (62 O.S. Supp. 2013,
10 Section 34.32), which relates to standard risk
11 assessments of state agencies; modifying requirement
12 for a state agency to conduct an information security
13 risk assessment; requiring risk assessment to be
14 conducted by a third party; providing exception for
15 certain state agencies; directing the Information
16 Services Division of the Office of Management and
17 Enterprise Services to approve certain number of
18 firms; requiring certain state agencies to submit a
19 final report; deleting certain penalty; deleting
20 criteria for risk assessments; amending 62 O.S. 2011,
21 Section 35.9, as last amended by Section 25, Chapter
22 358, O.S.L. 2013 (62 O.S. Supp. 2013, Section 35.9),
23 which relates to quarterly progress reports under the
24 Information Technology Consolidation and Coordination
Act; adding certain information to report; providing
an effective date; and declaring an emergency.

BE IT ENACTED BY THE PEOPLE OF THE STATE OF OKLAHOMA:

SECTION 1. AMENDATORY 62 O.S. 2011, Section 34.32, as
amended by Section 364, Chapter 304, O.S.L. 2012 (62 O.S. Supp.
2013, Section 34.32), is amended to read as follows:

Section 34.32 A. The Information Services Division of the
Office of Management and Enterprise Services shall create a standard

1 security risk assessment for state agency information technology
2 systems that complies with the International Organization for
3 Standardization (ISO) and the International Electrotechnical
4 Commission (IEC) Information Technology - Code of Practice for
5 Security Management (ISO/IEC ~~17799~~ 27002).

6 B. Each state agency that has an information technology system
7 shall ~~annually conduct~~ obtain an information security risk
8 assessment to identify vulnerabilities associated with the
9 information system. ~~A~~ Unless a state agency has internal expertise
10 to conduct the risk assessment and can submit certification of such
11 expertise along with the annual information security risk
12 assessment, the risk assessment shall be conducted by a third party.
13 The Information Services Division of the Office of Management and
14 Enterprise Services shall approve not less than two firms which
15 state agencies may choose from to conduct the information security
16 risk assessment. A state agency with an information technology
17 system that is not consolidated under the Information Technology
18 Consolidation and Coordination Act or that is otherwise retained by
19 the agency shall submit a final report of the information security
20 risk assessment ~~shall be submitted by each state agency~~ to the
21 Information Services Division by the first day of December of each
22 year. The final information security risk assessment report shall
23 identify, prioritize, and document information security
24 vulnerabilities for each of the state agencies assessed. ~~Failure to~~

1 ~~comply with the requirements of this subsection may result in~~
2 ~~funding being withheld from the agency. State agencies shall use~~
3 ~~either the standard security risk assessment created by the~~
4 ~~Information Services Division or a third-party risk assessment~~
5 ~~meeting the ISO/IEC 17799 standards and using the National Institute~~
6 ~~of Standards and Technology Special Publication 800-30 (NIST SP800-~~
7 ~~30) process and approved by the Information Services Division. The~~
8 ~~Information Services Division shall approve not less than two firms~~
9 ~~which state agencies may choose from to conduct the information~~
10 ~~security risk assessment.~~

11 C. The Information Services Division shall report the results
12 of the state agency assessments required pursuant to this section to
13 the Governor, the Speaker of the House of Representatives, and the
14 President Pro Tempore of the Senate by the first day of January of
15 each year.

16 SECTION 2. AMENDATORY 62 O.S. 2011, Section 35.9, as
17 last amended by Section 25, Chapter 358, O.S.L. 2013 (62 O.S. Supp.
18 2013, Section 35.9), is amended to read as follows:

19 Section 35.9 In addition to any other reporting requirements
20 required by law, the Chief Information Officer shall submit
21 quarterly progress reports to the Director of the Office of
22 Management and Enterprise Services, the Speaker of the House of
23 Representatives and the President Pro Tempore of the Senate. The
24 reports shall be submitted not later than January 31, April 30, July

1 31 and October 31 of each year and shall include, but not be limited
2 to, the following information:

3 1. The status of the implementation of the plan of action
4 required in paragraph 2 of subsection D of Section 34.11.1 of this
5 title;

6 2. A list of information technology assets and positions
7 transferred to the Information Services Division of the Office of
8 Management and Enterprise Services pursuant to the provisions of
9 subsection C of Section 35.5 of this title;

10 3. After July 1, 2012, and until the information technology
11 consolidation is completed, an annual reduction of three percent
12 (3%) in operational information technology and telecommunications
13 expenditures realized in the aggregate by all consolidated state
14 agencies;

15 4. A list of all state agencies which are not using the shared
16 services as required in Section 35.6 of this title;

17 5. A list of all exemptions or extensions granted pursuant to
18 the provisions of Section 35.7 of this title; ~~and~~

19 6. An accounting of the open source information technology
20 assets of the state, including a description of any new open source
21 assets deployed within the previous reporting period; and

22 7. Any other information as deemed appropriate by the Chief
23 Information Officer.

24 SECTION 3. This act shall become effective July 1, 2014.

